„De ce oare nimeni din cei ce au cunoscut tainele acestui domeniu nu l-a mai părăsit?“

În loc de introducere

“A scrie un proiect despre CRIPTOLOGIE pare, pentru cei ce cunosc domeniul, o încercare hazardată, datorită atît complexităţii cunoştinţelor pe care acesta le reclamă, vastităţii sale istorice si spaţiale (în toată lumea există asfel de preocupări), cît şi, mai ales, problematicii (de la simpla disimulare a înţelesului unui cuvânt până la metodele moderne de protecţie criptografică a depozitelor şi sistemelor de procesare a informaţiilor.

Cu ce să incepi şi la ce să te rezumi? Cum să organizezi materialul? Pentru cine să scrii: pentru specialişti, sau pentru publicul larg? Să încalci marele consemn al tăcerii celor ce au trudit aici, să dezvăluie cuceriri, fapte, întâmplări, împliniri şi neîmpliniri, oameni şi biografii, tehnici şi proceduri sau să faci doar ... aprecieri despre ...?

Senzaţia este asemănătoare cu cea pe care o trăieşti când pătrunzi într-un osuar sau intr-un templu. Nu ştii dacă ai voie doar să te mişti, să priveşti sau poţi să şi iscodeşti , nu ştii dacă ai voie să întrebi sau să descoşi, nu şti dacă, mai ales, poţi comenta, poţi emite judecăţi!

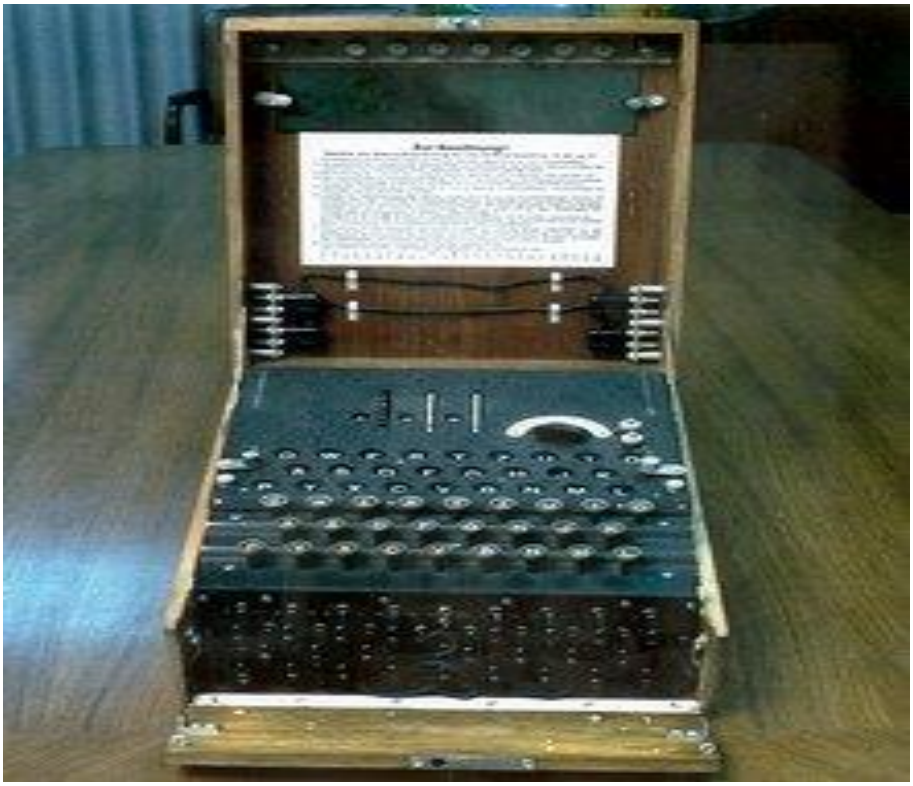
Ştii doar că ai datoria să înţelegi jertfa celor prezenţi cu fapta şi cu duhul şi să încerci să pui şi tu ceva acolo unde ei au pus totul.

Nu! Prin aceste gânduri nu am vrut să impresionăm, nu am dorit să facem obişnuita reclamă comercială pentru proiectul de faţă, ci doar să vă dezvăluim ce am simţit când am scris această „enigmă a enigmelor”.

Colonel ing. TĂNASE MIHAI
Colonel ing. GHEORGHE ILIE
Maior MIRCEA ANDRAŞIU

Maşina de criptat ENIGMA

Maşina Enigma este numele unei familii de maşini electromecanice criptografice cu rotoare utilizate pentru a genera cifruri pentru criptarea şi decriptarea de mesaje secrete. Enigma a fost folosită comercial de la începutul anilor 1920, fiind adoptată şi de armatele şi serviciile guvernamentale ale mai multor ţări–cel mai celebru caz fiind cel al Germaniei naziste înainte de şi în timpul celui de-al doilea război mondial.[1] Au fost produse, de-a lungul timpului, o varietate de modele diferite de Enigma, dar modelul armatei germane, **Wehrmacht Enigma**, este versiunea cel mai adesea studiată.



O maşină militară Germană Enigma. De jos în sus: tabela de prize, tastatura, lămpile şi roţile ce ies din interior şi se rotesc manual.

Maşina a căpătat notorietate deoarece criptologii aliaţilor au reuşit să decripteze un mare număr de mesaje care fuseseră cifrate cu această maşină. Decriptarea a devenit posibilă în 1932 datorită criptografilor polonezi Marian Rejewski, Jerzy Różycki şi Henryk Zygalski de la Biroul de Cifruri. La jumătatea lui 1939, metodele de reconstrucţie şi descifrare au fost prezentate

[1] Hakim, Joy(1995)(în engleză). A History of Us: War, Peace and all that Jazz. New York: Oxford University Press.

de Polonia Regatului Unit şi Franţei. Informaţiile obţinute din această sursă, denumite Ultra, au reprezentat un ajutor semnificativ pentru efortul de război al Aliaţilor. Influenţa exactă a Ultra nu este ştiută cu exactitate, dar o evaluare des întâlnită este cea că sfârşitul războiului din Europa a venit cu doi ani mai devreme datorită decriptării cifrurilor germane.[2][3]

Deşi cifrurile Enigma au slăbiciuni criptografice, în practică, doar în combinaţie cu alţi factori semnificativi (greşeli de operare, defecte procedurale, o maşină sau un caiet de coduri capturate ocazional) criptografii Aliaţilor au reuşit să descifreze mesajele.[4]

Maşina este dotată cu o tastatură prin care se introduce textul clar simbol cu simbol, iar la capătul celălalt (imprimantă sau tablu cu becuri) rezultă simbolurile criptate. Acestea sunt calculate în funcţie de starea rotoarelor (care se actualizează cu fiecare tastă apăsată), rotoare care controlează traseele circuitelor electrice de la intrare la ieşire. Versiunile iniţiale au fost simple, dar în mod constant s-au adăugat complicaţii la mecanism, pentru creşterea securităţii cifrului, cum ar fi creşterea numărului de rotoare şi adăugarea unui tablou de prize prin care se puteau substitui suplimentar perechi de simboluri.

Se mai păstrează încă maşini Enigma funcţionale, în muzee, unele chiar în stare de funcţionare, iar valoarea lor în licitaţii este de ordinul zecilor de mii de dolari. Rolul istoric al acestor maşini şi al criptanalizei lor a fost reflectat în unele lucrări artistice, mai ales în Polonia, ţară care a avut o contribuţie semnificativă la descifrarea mesajelor Enigma.

Desi cifrul Enigma are slabiciuni criptografice, practic nu asta a dus la spargerea codului ci alte intamplari "nefericite" ci capturarea de masini si caiete cu coduri, greseli ale operatorilor sau greseli procedurale.

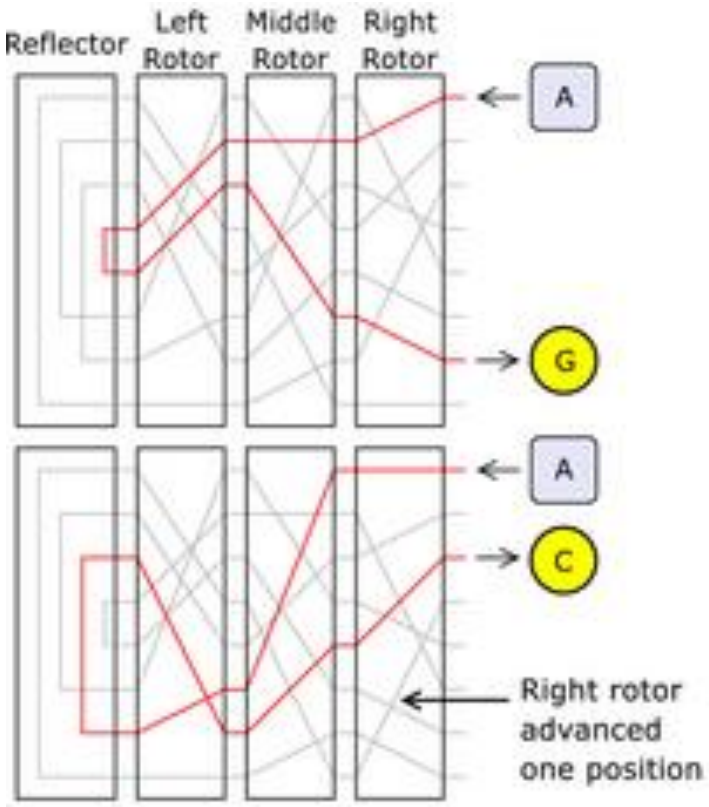
---

[2] Kahn(1991)

[3] Miller, A. Ray (2001). “The Cryptographic Mathematics of Enigma”. National Security Agency.

[4] Kahn(1991), Hinsley și Stripp (1993).

Descriere



*Encriptarea Enigma pentru doua litere consecutive- trece curent prin setul de rotoare prin reflector, si inapoi prin rotoare. Litera **A** se encripteaza diferit la doua apasari de taste diferite, mai intai in **G** si mai apoi in **C**. Asta este pentru ca rotorul din dreapta s-a miscat trimitand un semnal pe o cale complet diferita.*

Ca si alte masini cu rotoare, Enigma este o combinatie de sisteme mecanice si electrice. Mecanismul mecanic consta intr-o tastatura, un set de discuri rotative numite **rotoare** si un mecanism de deplasare care ajuta la miscarea unuia sau a mai multe discuri atunci cand o tasta este apasata. Exista mai multe tipuri de mecanisme, dar cel mai comun este cel pentru care rotorul de mana dreapta se misca pentru fiecare apasare de tasta si ocazional miscarea rotoarelor vecine este provocata. Miscarea continua a rotoarelor duce la o transformare criptografica diferita la fiecare apasare de tasta.

Partile mecanice se comporta in asa fel incat sa se formeze un circuit electric diferit- encriptarea propriu-zisa a unui caracter este facuta electronic. Cand o tasta este apasata, circuitul se completeaza; curent electric circula prin componente si in final lumineaza una din lampi, indicand litera de iesire. De exemplu, cand se incepe criptarea unui mesaj operatorul va putea apasa intai

tasta **A** si lampa **Z** s-ar putea aprinde, devenind prima litera din mesajul criptat. Criptarea va continua in acelasi fel.

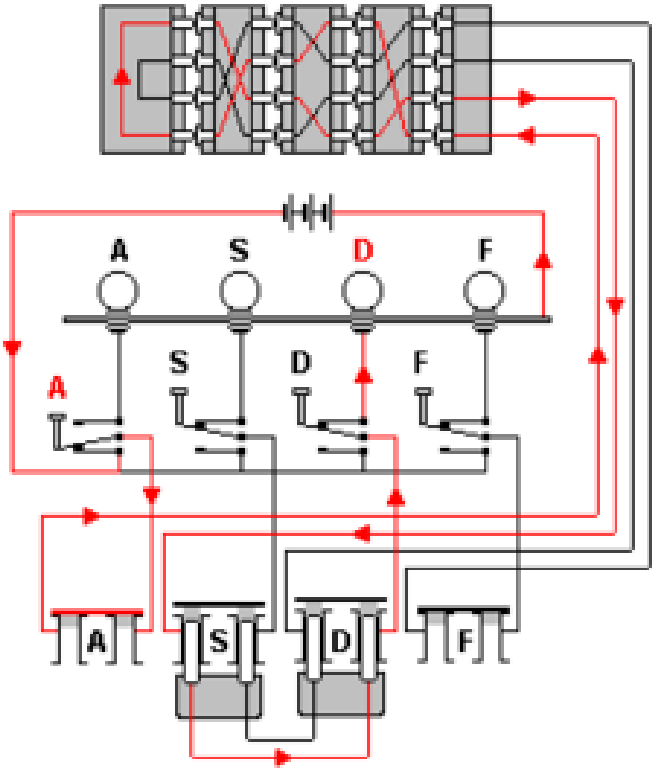


*Diagrama completa a rotirii este aratata in diagrama de mai sus unde fluxul electric cand se apasa tasta **A** aprinde lampa **D**.*

Curentul electric porneste de la o **sursa** printr-un **intrerupator** bidirectional controlat de tasta eliberata. Tabela de prize faciliteaza conexiunea intre tastatura si "roata de intrare" fixata putand fi usor refacuta de catre un alt operator. Din tabela de intreruperi curentul electric trece in "roata de intreare" fixata. De aici in ansamblul de rotoare, unde structura complexa a fiecarui rotor duce la circularea foarte schimbatoare a curentului electric de la un rotor la urmatorul. Dupa strabaterea tuturor rotoarelor, circuitul continua prin "reflector", care respinge semnalul din nou prin rotoare si "roata de intrare"- pe alta cale de aceasta data- si trece prin prize si prin intrerupatorul bidirectional a literei tinta si aprinde lampa potrivita.

Rotoarele

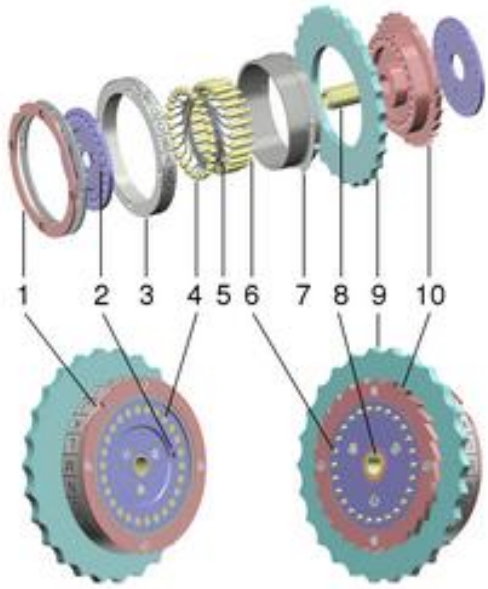
Un rotor Enigma

Rotoarele (numite şi *roţi* sau *tamburi—Walzen* în germană) formează inima unei maşini Enigma. De aproximativ 10 cm în diametru, fiecare rotor este un disc din cauciuc tare sau din bachelită cu o serie de ace de bronz cu arc pe o parte aranjate în cerc; pe cealaltă parte sunt un număr corespunzător de contacte electrice circulare. Acele şi contactele reprezintă alfabetul–de regulă cele 26 de litere A–Z. Când sunt plasate unul lângă altul, acele unui rotor se sprijină pe contactele rotorului vecin, formând o conexiune electrică. Înăuntrul unui rotor, un set de 26 de fire conectează fiecare ac de pe o parte cu un contact din partea cealaltă într-un şablon complex. Cablajele diferă pentru fiecare tablou.

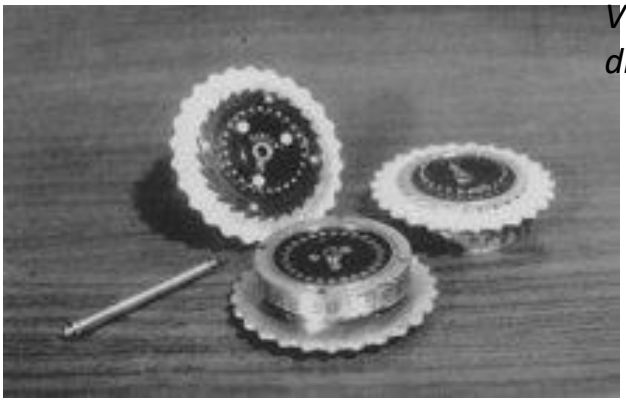
Individual, un rotor efectuează doar un tip foarte simplu de criptare–un cifru cu substituţie simplu. De exemplu, acul corespunzător literei E ar putea fi cablat cu contactul pentru litera T de pe partea opusă. Complexitatea provine de la utilizarea mai multor rotoare în serie—de regulă trei sau patru—şi de mişcarea regulată a rotoarelor; aceasta furnizează un tip de criptare mult mai puternic.

În cadrul unei maşini, un rotor poate fi setat pe una din 26 de poziţii. Aceasta se poate face manual cu ajutorul unui potenţiometru, aşa cum se arată în figura 2. Ca operatorul să cunoască poziţia, fiecare rotor are un *inel alfabetic* ataşat pe exteriorul discului, cu 26 de litere sau numere; una dintre acestea se vede printr-o fereastră, indicând operatorului poziţia rotorului. La primele modele Enigma, inelul alfabetic era fix; o complicaţie introdusă în versiunile ulterioare o reprezintă facilitatea de a ajusta inelul alfabetic relativ la cablarea din centru.

Poziţia inelului este cunoscută sub denumirea de *Ringstellung* („setarea inelului”).



Trei rotoare in interiorul Enigmei



Trei rotoare Enigma si axul pe care sunt fixate

Versiune expandata a unui rotor din Enigma

1. inel crestat
2. punct marcant pentru contactul A
3. inelul cu alfabetul (fabricat din cauciuc)
4. contacte
5. conexiuni
6. pin contacts
7. parghie ajustabila, declansata de un arc
8. butuc
9. roata actionata manual
10. roata zimtata

Rotoarele conţin fiecare unul sau mai multe marcaje, utilizate pentru a controla succesiunea de stări ale rotoarelor. În versiunile militare, marcajele se află pe inelul alfabetic.

Enigma Armatei şi a Forţelor Aeriene erau echipate cu câteva rotoare; la început au fost doar trei. la 15 decembrie 1938 numărul a crescut la cinci, dintre care trei erau alese pentru introducerea în maşină. Acestea erau marcate cu cifre romane: I, II, III, IV şi V, fiecare cu câte un singur marcaj aflat în diferite puncte ale inelului alfabetic. Intenţia a fost ca aceasta să fie o măsură de securitate, dar în cele din urmă s-a dovedit a fi o slăbiciune ce a permis atacurile ceasului (efectuat de polonezi) şi Banburismus (al britanicilor).

Versiunea navală a maşinii Enigma utilizată de Wehrmacht a avut mereu mai multe rotoare decât celelalte servicii: la început, şase, apoi şapte şi în cele din urmă opt. Rotoarele suplimentare, numerotate VI, VII şi VIII, aveau toate cablaje diferite, şi două marcaje tăiate în ele la N şi A, având ca rezultat o modificare mai frecventă.

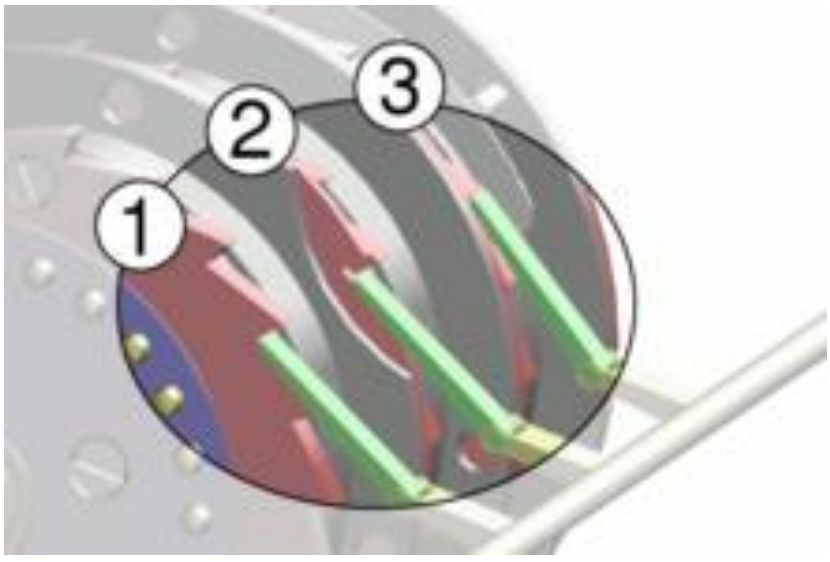
Maşina Enigma cu patru rotoare (M4) a Marinei Germane avea un rotor în plus într-un volum egal cu cel din versiunea cu trei rotoare. Aceasta s-a realizat prin înlocuirea reflectorului original cu unul mai subţire şi adăugarea unui al patrulea rotor special. Al patrulea rotor poate fi unul din două tipuri, „Beta” sau „Gamma”, şi nu îşi schimbă niciodată starea, putând fi pus manual în oricare din cele 26 de poziţii.

Schimbarea de stare

Pentru a evita implementarea doar a unui simplu (şi slab) cifru cu substituţie, unele rotoare se roteau la apăsările consecutive ale unei taste. Aceasta asigura că substituţia criptografică va fi diferită la fiecare simbol, având ca rezultat o cifru cu substituţie polialfabetică.

Cel mai adesea, acest scop este îndeplinit cu ajutorul unui clichet. Fiecare rotor are o roată dinţată cu 26 de dinţi; un grup de opritoare sprijină aceşti dinţi. Acestea avansau la unison cu fiecare apăsare de tastă. Dacă un opritor ajunge la un dinte al roţii, acel rotor îşi schimbă starea.

În Enigma Wehrmacht, fiecare rotor avea un inel ajustabil. Cele cinci rotoare elementare (I–V) aveau fiecare câte un marcaj, iar cele ale maşinii navale VI, VII şi VIII aveau câte două. La un anumit moment, marcajul unui rotor ajunge să fie aliniat cu opritorul, permiţându-i să acţioneze clichetul următorului rotor la următoarea apăsare de tastă. Când un opritor nu este aliniat cu marcajul, el doar alunecă puţin pe suprafaţa inelului fără a acţiona roata dinţată. Într-un sistem de rotoare cu un singur marcaj, al doilea rotor avansează cu o poziţie la fiecare 26 de avansuri ale primului rotor. Analog, al treilea rotor avansează cu o poziţie la fiecare 26 de avansuri ale celui de-al doilea rotor. Al doilea rotor avansează şi el împreună cu al treilea, ceea ce înseamnă că al doilea rotor poate face doi paşi la apăsarea de taste—„pasul dublu”—având ca rezultat o reducere a perioadei.[5]



Schimbarea stărilor maşinii Enigma

Acest pas dublu cauzează devierea rotoarelor de comportamentul unui odometru obişnuit. Un pas dublu are loc după cum urmează: primul rotor avansează, şi împinge al doilea rotor un pas mai departe. Dacă al doilea rotor se mişcă la acest pas în poziţia marcajului său, al treilea clichet cade. La pasul următor, acest clichet împinge roata dinţată a celui de-al treilea rotor, trecând în marcajul celui de-al doilea rotor, mişcându-l şi pe acesta a doua oară consecutiv.

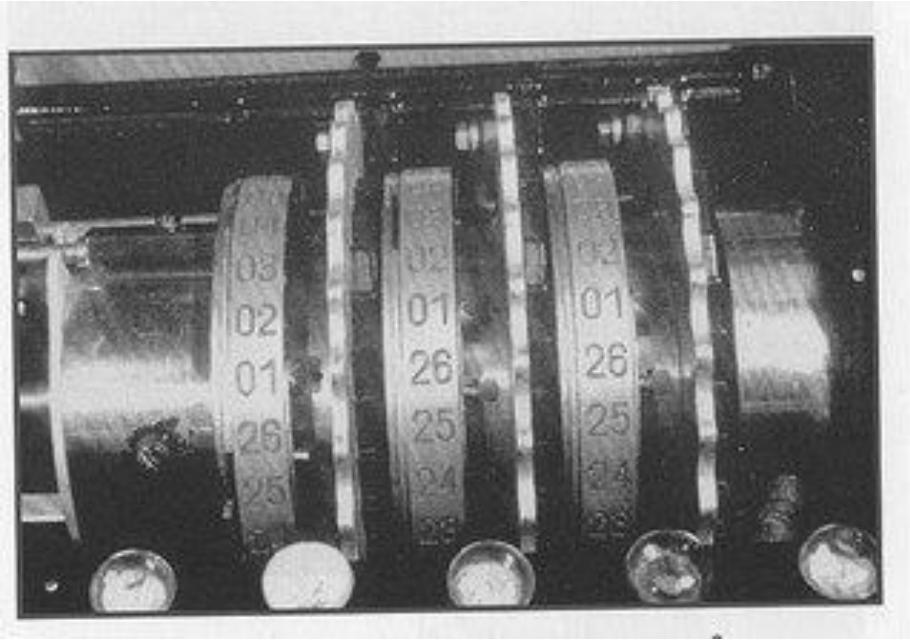
Cu trei roţi şi un singur marcaj în prima şi a doua roată, maşina are o perioadă de 26 × 25 × 26 = 16.900 (în loc de 26 × 26 × 26, din cauza pasului dublu al celui de-al doilea rotor.[5]) Istoric, dimensiunea mesajelor era limitată la numere de ordinul sutelor de litere, astfel existând un risc redus de repetare a unei poziţii în cadrul unui singur mesaj.

Pentru a face loc pentru rotorul numărul patru, „Beta" respectiv „Gamma", introduse în 1942, reflectorul a fost schimbat, făcându-l mai subţire şi al patrulea rotor special, şi el mai subţire, a fost pus lângă el. În restul mecanismului, nu s-a produs nicio schimbare. Deoarece existau doar trei clichete, al patrulea rotor nu avansa niciodată, dar putea fi pus manual într-una din cele 26 de poziţii.

La apăsarea unei taste, rotoarele avansau înainte de conectarea circuitului electric.

[5] David Hamer, „Enigma: Actions Involved in the 'Double-Stepping' of the Middle Rotor" , Cryptologia, 21(1), ianuarie 1997, pag 47-50

Roata de intrare



Ansamblul de rotoare din Enigma. Cele trei rotoare mobile sunt prinse intre doua roti fixe: roata de intrare in dreapta si reflectorul in stanga.

Roata de intrare (în germană *Eintrittswalze*), sau statorul de intrare, conectează tabloul de prize, sau, dacă acesta nu există, tastatura şi tabloul de tabloul de lămpi, cu ansamblul rotoarelor. Deşi cablarea exactă utilizată este de importanţă redusă pentru nivelul de securitate, s-a dovedit totuşi a fi un obstacol pentru criptanalistul polonez Marian Rejewski în încercarea sa de a deduce cablajul rotoarelor. Maşina Enigma comercială conectează tastele în ordinea secvenţei lor pe tastatură: Q→A, W→B, E→C şi aşa mai departe. Însă maşina Enigma militară le conectează în ordine alfabetică
directă: A→A, B→B, C→C etc. A fost nevoie de o bănuială foarte inspirată a lui Rejewski pentru a descoperi modificarea, iar după aceasta, el a reuşit să rezolve şi mai inspiratele sale ecuaţii.

Reflectorul

Cu excepţia primelor modele A şi B, ultimul rotor se afla înainte de un *reflector* (în germană *Umkehrwalze*, adică „roată de inversare”), o piesă patentată, care deosebea familia de maşini Enigma de diferitele maşini cu rotor proiectate în acea perioadă. Reflectorul conectează ieşirile ultimelor rotoare în perechi, redirecţionând curentul electric înapoi prin rotoare pe un canal diferit. Reflectorul asigură că transformarea operată de Enigma este propria sa inversă: astfel, criptarea şi decriptarea sunt aceeaşi operaţie şi este efectuată de acelaşi mecanism. Dar reflectorul i-a dat maşinii Enigma şi proprietatea că nicio literă nu era vreodată transformată în ea însăşi. Aceasta a reprezentat un defect conceptual grav şi o greşeală criptografică exploatată ulterior de criptanalişti.

În modelul C, reflectorul putea fi inserat într-una din două poziţii diferite. În modelul D, reflectorul putea fi setat în 26 de poziţii posibile, deşi nu se putea mişca în timpul criptării. În Enigma Abwehr, reflectorul îşi schimba starea în timpul criptării, ca şi celelalte roţi.

În maşina Enigma a armatei germane şi a forţelor aeriene, reflectorul era fix şi nu se rotea; au existat patru versiuni. Cea originală denumită *A* a fost înlocuită de *Umkehrwalze B* la 1 noiembrie 1937. O a treia versiune, *Umkehrwalze C* a fost utilizată pentru scurt timp în 1940, probabil din greşeală, şi a fost spartă de Hut 6.[6] Cea de-a patra versiune, observată prima oară la 2 ianuarie 1944 avea un reflector recablabil, numit *Umkehrwalze D*, care permitea operatorului maşinii Enigma să includă modificarea conexiunilor ca parte din cheie.

---

[6] Philip Marks, „Umkerhrwalze D.: Enigma’s Rewieable Reflector – Part I”, Cryptologia 25(2), April 2001, pag 101 - 141

Tabela de prize

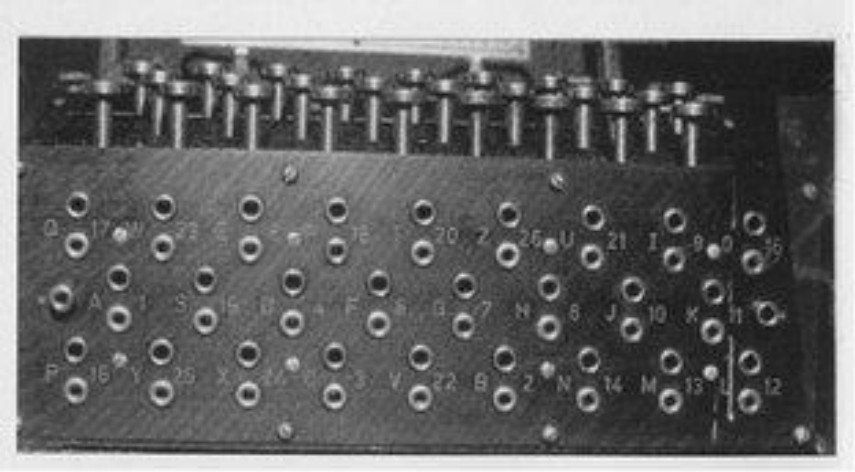


Tabela de prize (Steckerbrett), aici fara cabluri conectate, este amplasata in partea frontala a masinii, sub tastatura. In timpul utilizarii se pot face pana la 13 conexiuni pe tabela.

Tabloul de prize (în germană *Steckerbrett*) permitea o cablare variabilă ce putea fi reconfigurată de operator (după cum se vede pe panoul frontal al figurii 1; unele din cablurile de conectare se văd în capac). A fost introdus în versiunea armatei germane în 1930 şi a fost adoptat şi de Marină curând după aceea. Tabloul de prize contribuia semnificativ la puterea criptării maşinii, mai mult decât ar fi făcut-o un rotor suplimentar. Enigma fără tablou de prize poate fi rezolvată relativ uşor folosind metode manuale; aceste tehnici sunt însă învinse prin adăugarea tabloului, iar criptanaliştii Aliaţilor au recurs la maşini speciale pentru a rezolva problema.

Un cablu pus pe panoul de prize conectează o pereche de litere între ele, de exemplu, E şi Q ar putea fi o pereche conectată. Efectul conexiunii era interschimbarea celor două litere înainte şi după unitatea criptografică principală, cu rotoare. De exemplu, când un operator apasă E, semnalul este deviat spre Q înainte de a intra în rotoare. Un număr de până la 13 astfel de perechi puteau fi folosite simultan.

Curentul trecea dinspre tastatură spre tabloul de prize şi mai departe spre rotorul de intrare (*Eintrittswalze*). Fiecare literă de pe tabloul de prize are două intrări. Introducerea unei mufe deconecta intrările superioară (dinspre tastatură) şi cea inferioară (spre rotorul de intrare) ale acelei litere. Mufa de la celălalt capăt al cablului era introdusă în intrarea altei litere, schimbând conexiunile între ele.

Accesorii

"Schreibmax" era o unitate de listat care era atasata Enigmei, salvandu-se literele ce se aprindeau pe tabela cu lampi.

Un accesoriu utilizat de Enigma M4 a fost „Schreibmax”, o mică imprimantă care tipărea cele 26 de litere pe o mică bandă de hârtie. Aceasta a eliminat necesitatea ca un al doilea operator să citească lămpile şi să noteze literele textului cifrat. Schreibmax era pus peste maşina Enigma şi era conectat la panoul de lămpi. Pentru a instala imprimanta, carcasa lămpilor şi toate becurile trebuiau demontate. În pofida acestui inconvenient, ea putea îmbunătăţi securitatea operaţională; imprimanta putea fi instalată la distanţă astfel încât ofiţerul care opera maşina nu mai trebuia să vadă informaţia decriptată (textul clar).

Un alt accesoriu al maşinii era panoul de lămpi la distanţă. Dacă maşina era echipată cu un panou suplimentar, carcasa de lemn era mai mare pentru a-l putea conţine. Exista o versiune de panou de lămpi ce putea fi conectat după aceea, dar care necesita, ca şi Schreibmax, ca panoul de lămpi şi becurile să fie scoase. Panoul de la distanţă făcea posibil ca o persoană să citească textul decriptat fără ca operatorul să-l citească.

Ataşamentul Uhr

În 1944, Luftwaffe a introdus un comutator suplimentar pe tabloul de prize, comutator numit Uhr (ceas). Era o cutie mică ce conţinea un comutator cu 40 de poziţii. El înlocuia prizele iniţiale. După conectarea prizelor, aşa cum se arăta în foaia zilnică de chei, operatorul punea comutatorul într-una din cele 40 de poziţii, fiecare producând o altă combinaţie de cablaje. Majoritatea acestor conexiuni nu erau pe perechi. Într-o singură poziţie a comutatorului, Uhr nu făcea decât să emuleze 9 conexiuni realizate pe panoul de prize.

Descriere matematica

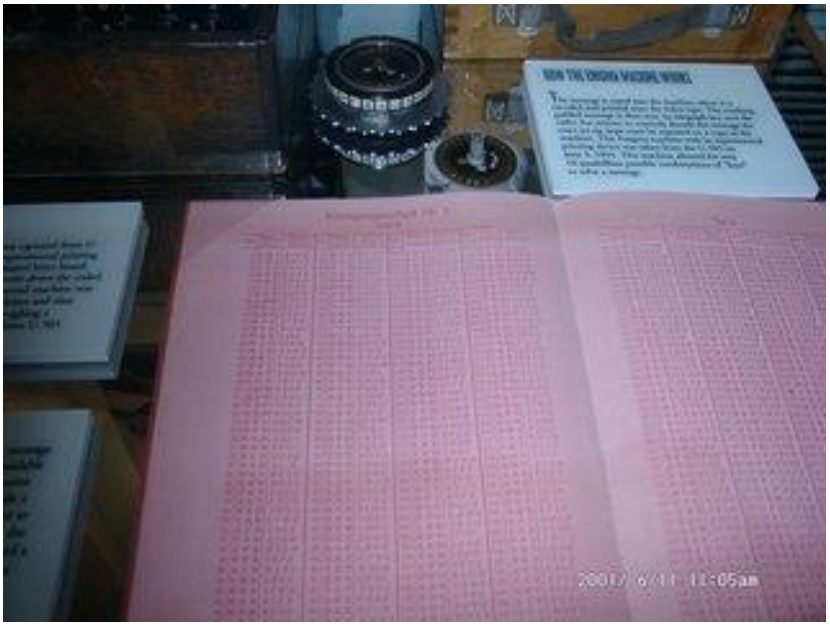
Transformarea Enigma pentru fiecare literă poate fi specificată matematic ca un produs de permutări. Presupunând o maşină Enigma a armatei germane sau a forţelor aeriene, fie *P* transformarea tabloului de prize, *U* cea dată de reflector, şi *L*,*M*,*R* respectiv cele date de cele trei rotoare. Atunci criptarea *E* poate fi exprimată ca:

$$E = PRMLUL^{-1}M^{-1}R^{-1}P^{-1}.$$

La fiecare apăsare de tastă, rotoarele se modifică, schimbând transformarea. De exemplu, dacă rotorul din dreapta *R* este rotit cu *i* poziţii, transformarea devine $\rho^{i}R\rho^{-i}$, unde ρ este permutarea ciclicăce transformă A în B, B în C, şi aşa mai departe. Analog, rotoarele stâng şi central pot fi reprezentate ca rotaţiile de *j* şi *k* ale lui *M* şi *L*. Transformarea de criptare poate fi descrisă ca:

$$E = P(\rho^{i}R\rho^{-i})(\rho^{j}M\rho^{-j})(\rho^{k}L\rho^{-k})U(\rho^{k}L^{-1}\rho^{-k})(\rho^{j}M^{-1}\rho^{-j})(\rho^{i}R^{-1}\rho^{-i})P^{-1}.$$

Proceduri de folosire a Enigmei



In timp ce era folosita Enigma avea nevoie de o lista de setari zilnice a tastelor si de un numar de documente auxiliare. Procedurile marinei germane au fost cele mai elaborate. Caietele de coduri ale marinei erau scriese cu rosu, cu cerneala solubila, erau deci usor de distrus daca erau capturate. caietul de sus a fost luat dintr-un submarin capturat(U-505).

În armata germană, comunicaţiile erau împărţite într-un număr de reţele diferite, toate cu setări diferite pentru maşinile lor Enigma. Aceste reţele de comunicaţii erau numite la Bletchley Park *chei*, şi aveau asignate câte un nume de cod, cum ar fi *Red* (*Roşu*), *Chaffinch* (*Cinteza*) şi *Shark* (*Rechinul*). Fiecare unitate care opera pe o reţea primea o listă de setări pentru maşinile Enigma, valabilă o perioadă de timp. Pentru ca un mesaj să fie corect criptat şi decriptat, atât transmiţătorul cât şi receptorul trebuiau să-şi seteze maşina Enigma în acelaşi fel; selecţia şi ordinea rotoarelor, poziţia de pornire şi conexiunile de pe tabloul de prize trebuia să fie identice. Toate aceste setări (care împreună formau, în termeni moderni, cheia) trebuia să fi fost stabilite anterior, şi erau distribuite în cărţi de coduri.

Starea iniţială a unei maşini Enigma avea câteva aspecte:

- Ordinea roţilor (*Walzenlage*)—alegerea rotoarelor şi ordinea în care sunt ele montate.
- Poziţia iniţială a rotoarelor—aleasă de operator, diferită de la mesaj la mesaj.
- Setările inelelor (*Ringstellung*)—poziţia inelelor alfabetice relativ la cablarea rotoarelor.
- Setările prizelor (*Steckerverbindungen*)—conexiunile prizelor de pe tablou.
- În versiunile cele mai recente, cablarea reflectorului reconfigurabil.

Enigma a fost proiectată să fie sigură chiar şi dacă este cunoscută cablarea rotoarelor de către adversar, deşi în practică s-au depus eforturi considerabile pentru a o păstra şi pe aceasta secretă. Dacă cablarea e secretă, numărul total de configuraţii posibile a fost calculat a fi de ordinul a 10^{114} (aproximativ 380 biţi); când cablajul este cunoscut şi cu alte constrângeri operaţionale, dimensiunea spaţiului este redusă la ordinul a 10^{23} (76 biţi).[3] Utilizatorii Enigma erau încrezători în securitatea sa din cauza numărului mare de posibilităţi; la acea vreme, nu era fezabil ca un adversar să înceapă măcar să încerce fiecare configuraţie posibilă într-un atac cu forţă brută.

Indicatori

Cu capacul lasat, Enigma este gata de utilizare. Rotile ce patrund prin capac permit operatorului sa regleze manual rotoarele. Pozitia curenta-aici-`RDKP` — este vizibila operatorului printr-un set de capace transparente.

Majoritatea cheilor erau păstrate în vigoare o anumită perioadă de timp, de regulă o zi. Totuşi, o poziţie iniţială diferită a rotorului era aleasă pentru fiecare mesaj, concept similar cu cel de vector de iniţializare din criptografia modernă, deoarece dacă mai multe mesaje sunt trimise criptat cu setări aproape identice, atunci un criptanalist, folosind mai multe mesaje interceptate, ar putea ataca mesajele folosindu-se de analiza frecvenţei. Poziţia iniţială era transmisă chiar înainte de textul cifrat. Metoda exactă utilizată era denumită "procedura de indicator"—slăbiciunile acestei proceduri au deschis calea primelor spargeri ale maşinii Enigma.

Unele din primele proceduri de indicator a fost utilizată de criptanaliştii polonezi pentru a reuşi primele spargeri cu succes ale maşinii Enigma. Procedura era ca operatorul să-şi seteze maşina în conformitate cu lista de setări, care includea o poziţie iniţială globală a rotoarelor (*Grundstellung*), de exemplu AOH. Operatorul întorcea rotoarele până când literele AOH apăreau prin geamuri. În acel punct, operatorul îşi alegea o poziţie de start arbitrară pentru mesajul respectiv. Putea alege de exemplu EIN, iar aceasta devenea *setarea de mesaj* pentru acea sesiune de criptare. Operatorul scria

atunci EIN la tastatura maşinii, de două ori, pentru a permite detecţia erorilor de transmisie. Rezultatul era un indicator criptat— EIN scris de două ori s-ar fi putut transforma de exemplu în XHTLOA, care ar fi transmis împreună cu mesajul. În cele din urmă, operatorul punea rotorul la setarea de mesaj, EIN în acest exemplu, şi scria textul clar al mesajului.

La capătul celălalt, operation era inversată. Operatorul seta maşina la valorile iniţiale şi scria primele şase litere ale mesajului (XHTLOA). În acest exemplu, lămpile ar fi arătat EINEIN. Mutând rotoarele pe EIN, operatorul receptor scria apoi restul textului cifrat, descifrând mesajul.

Slăbiciunea acestei scheme de indicator venea din două surse. În primul rând, din utilizarea unei setări globale de iniţializare—aceasta a fost ulterior schimbată, astfel încât operatorul îşi selecta valoarea iniţială pentru a cripta indicatorul, şi trimitea poziţia iniţială în clar. A doua problemă era repetiţia indicatorului, un defect grav de securitate. Setarea mesajului era codificată de două ori, având ca rezultat o relaţie între prima şi a patra, a doua şi a cincea, respectiv a treia şi a şasea literă. Această problemă de securitate a permis Biroului de Cifruri din Polonia spargerea sistemului Enigma dinainte de război încă din 1932. Totuşi, după 1940, germanii au schimbat procedurile pentru a îmbunătăţi securitatea.

În timpul celui de-al doilea război mondial, s-au folosit cărţi de coduri doar pentru setarea rotoarelor şi a inelelor. Pentru fiecare mesaj, operatorul alegea o poziţie aleatoare de pornire, să zicem WZA, şi o cheie aleatoare de mesaj, de exemplu SXT. Apoi muta rotoarele în poziţia de start WZA şi codifica cheia mesajului SXT. Presupunând că mesajul rezultat era UHL, el îşi seta apoi cheia de mesajSXT ca poziţie de start şi cripta mesajul. Apoi, transmitea poziţia de start WZA, cheia mesajului UHL şi apoi textul cifrat. Receptorul seta poziţia de start conform primei trigrame, WZA şi apoi decodifica a doua trigramă, UHL, pentru a obţine setarea de mesaj SXT. Apoi, utiliza acest SXT ca poziţie de start pentru a decripta mesajul. Astfel, fiecare setare iniţială era diferită şi noua procedură evita defectul de securitate dat de dubla codificare a setărilor de mesaj.

Această procedură a fost utilizată doar de Wehrmacht şi de Luftwaffe. Procedurile Kriegsmarine de la transmiterea mesajelor cu Enigma mult mai elaborate şi complexe. Înainte de criptarea cu Enigma, mesajele erau codificate cu ajutorul cărţii de coduri Kurzsignalheft. Kurzsignalheft conţinea tabele de conversie ale diferitelor propoziţii în grupuri de câte patru litere. Erau incluse numeroase posibilităţi, cum ar fi chestiuni logistice cum ar fi realimentarea cu combustibil sau întâlnirea cu navele de provizii, poziţii, nume de porturi, ţări, arme, starea vremii, poziţiile şi navele inamice, tabele de date şi ore. O altă carte de coduri conţinea *Kenngruppen* şi *Spruchschlüssel*: identificarea cheii şi cheile de mesaj.

Abrevieri şi moduri de lucru

Maşina Enigma a armatei utiliza doar cele 26 de caractere alfabetice. Semnele erau înlocuite de combinaţii rare de caractere. Spaţiul era omis şi înlocuit cu X. X era în general folosit ca punct. Unele semne erau diferite în alte părţi ale armatei. Wehrmachtul a înlocuit virgula cu ZZ şi semnul de întrebare cu FRAGE sau FRAQ. Kriegsmarine însă, a înlocuit virgula cu Y şi semnul de întrebare cu UD. Combinaţia CH, ca în cuvântul "acht" (opt) sau "Richtung" (direcţie) au fost înlocuite cu Q (AQT, RIQTUNG). Două, trei sau patru zerouri erau înlocuite cu CENTA, MILLE şi MYRIA.

Wehrmacht şi Luftwaffe transmiteau mesajele în grupuri de câte patru caractere. Kriegsmarine, utilizând maşina Enigma cu patru rotoare, avea grupuri de patru caractere. Numele sau cuvintele folosite des erau variate atât cât se putea. Cuvinte ca Minensuchboot (detector de mine) puteau fi scrise MINENSUCHBOOT, MINBOOT, MMMBOOT sau MMM354. Pentru a îngreuna criptanaliza, era interzisă transmiterea de mesaje de peste peste 250 de caractere. Mesajele mai lungi erau împărţite în mai multe părţi, fiecare cu propria sa cheie de mesaj. Pentru mai multe detalii, vezi traducerile lui Tony Sale ale „Procedurii generale”[7] şi ale „Procedurii pentru ofiţeri şi personal”.[8]

[7] “The translated 1940 Enigma General Procedure”

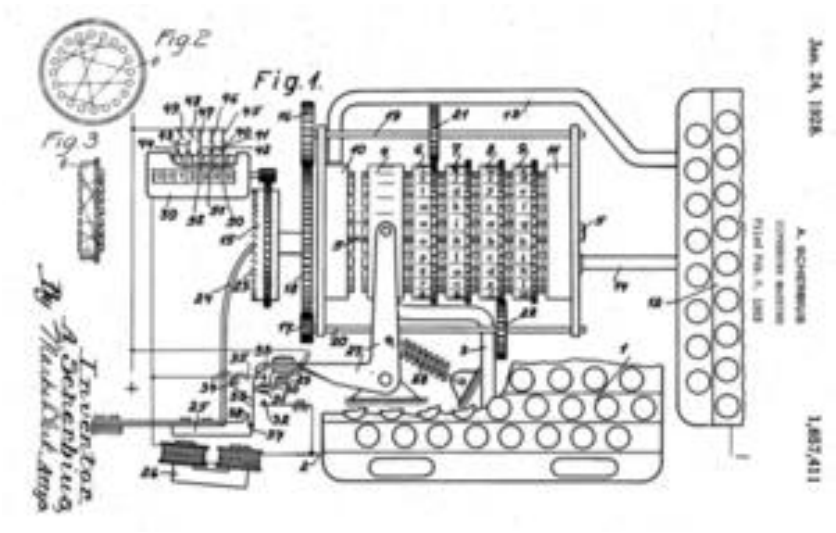
[8] „The translated 1940 Enigma Offizier and Staff Procedure”

Istoria şi dezvoltarea maşinii

Au existat numeroase modele şi variante ale familiei Enigma. Primele maşini Enigma erau modele comerciale de la începutul anilor 1920. Începând de la jumătatea acelui deceniu, diferitele ramuri ale armatei germane au început să folosească Enigma, efectuând un număr de modificări pentru a-i creşte nivelul de securitate. În plus, mai multe alte ţări au adoptat sau au adaptat designul Enigma pentru propriile lor maşini de cifrare.

O selecţie de şapte maşini Enigma şi echipament auxiliar, expuse la Muzeul Criptologic Naţional din SUA. De la stânga la dreapta, modelele sunt: 1) Enigma comercială; 2) Enigma T; 3) Enigma G; 4) Model neidentificat; 5) Enigma Luftwaffe (forţele aeriene); 6) Enigma Heer (a armatei); 7) Enigma M4 a Kriegsmarine.

Enigma "comerciala"



Patentul Scherbius' Enigma — USA #1,657,411, eliberat in 1928

La 23 februarie 1918, inginerul german Arthur Scherbius a depus o cerere de patent pentru o maşină de cifrare cu rotoare şi, împreună cu E. Richard Ritter, a fondat firma Scherbius & Ritter. Ei au abordat marina germană şi ministerul de externe pentru a le prezenta proiectul, dar nu au găsit interes pentru acesta. Apoi ei au dat drepturile asupra patentului firmei Gewerkschaft Securitas, care a fondat Chiffriermaschinen Aktien-Gesellschaft (Societatea pe Acţiuni Maşini de Cifrare) la 9 iulie 1923; Scherbius şi Ritter făceau parte din consiliul director.

Chiffriermaschinen AG a început să facă reclamă unei maşini cu rotoare—*Enigma model A*—care a fost expusă la Congresul Uniunii Poştale Internaţionale în 1923 şi în 1924. Maşina era grea şi masivă, şi conţinea şi o maşină de scris. Măsura 65×45×35 cm şi cântărea aproximativ 50 kg. A fost introdus şi un *model B,* cu o construcţie similară.[9] Deşi şi ele au purtat numele de Enigma, atât modelul A cât şi modelul B erau diferite de versiunile ulterioare: atât forma şi mărimea, cât şi funcţionalitatea, prin aceea că lor le lipsea reflectorul.

Reflectorul—o idee propusă de colegul lui Scherbius Willi Korn—a fost introdusă prima oară în modelul *Enigma C* (1926). Reflectorul este o piesă-cheie a maşinilor Enigma.

---

9 “Imagine cu Enigma B”

Exemplar rar de maşină Enigma cu 8 rotoare şi imprimantă.

Modelul C era mai mic şi mai portabil decât predecesoarele sale. Îi lipsa maşina de scris, bazându-se în schimb pe citirea de către operator a lămpilor; astfel, modelul a fost numit "Enigma cu lămpi" pentru a-l distinge de modelele A şi B. Enigma C a dispărut rapid, făcând loc modelului *Enigma D* (1927). Această versiune a fost folosită pe scară largă, în Suedia, Olanda, Regatul Unit, Japonia, Italia, Spania, Statele Unite şi Polonia.

Enigma "militara"

Marina a fost prima ramură a armatei germane care a adoptat Enigma. Această versiune, numită *Funkschlüssel C* (*Cifru radio C*), a fost pusă în producţie până în 1925 şi a fost introdusă în folosinţă în 1926.[10] Tastatura şi tabloul de lămpi conţineau 29 de litere—de la A la Z, Ä, Ö şi Ü—aranjate în ordine alfabetică, şi nu în ordinea QWERTZU.[11] Rotoarele aveau 28 de contacte, litera X fiind cablată să treacă necriptată prin rotoare.[12] Trei rotoare erau alese dintr-un set de cinci[13] şi reflectorul putea fi introdus în una din patru poziţii diferite, notate α, β, γ şi δ.[14] Maşina a fost revizuită în iulie 1933.[15]

Masini Enigma la muzeul Criptologic National SUA

Până la 15 iulie 1928,[16] armata germană (*Reichswehr*) îşi introdusese propria sa versiune de Enigma—*Enigma G*, urmată de versiunea sa revizuită *Enigma I* până în iunie 1930.[17] Enigma I este numită şi

---

[10] Khan, 1991, pag. 39-41, 299

[11] Ulbrich, 2005, pag 4

[12] Stripp, 1993

[13] Khan, 1991, pag 40, 299

[14] Bauer, 2000, pag 108

[15] Hinsley and Stripp, 1993

[16] Kahn, 1991, pag 41, 299

[17] Deavours and Kruh, 1985, pag 97

Enigma *Wehrmacht*, sau *Servicii*, şi a fost utilizată de serviciile militare germane şi de alte organizaţii guvernamentale (cum ar fi căile ferate[18]), înaintea şi în timpul celui de-al doilea război mondial. Diferenţa majoră dintre Enigma I şi modelele comerciale a fost adăugarea tabloului de prize pentru a schimba între ele perechi de litere, mărind cu mult puterea criptografică a maşinii. Printre alte diferenţe se numărau utilizarea unui reflector fix, şi mutarea marcajelor de schimbare a stării de pe corpul rotorului pe inelele mobile cu litere.[17] Maşina măsura 28×34×15 cm şi cântărea în jur de 12 kg.[12]

Un model T de Enigma (Tirpitz) — un model comercial Enigma K fabricata pentru japonezi.

Până în 1930, Armata a sugerat ca şi Marina Militară să adopte această maşină, arătând beneficiile sporului de securitate (cu tabloul de prize) şi simplificarea comunicaţiilor între servicii.[19] Marina a acceptat în cele din urmă şi în 1934[20] au introdus versiunea specială a maşinii armatei, denumită *Funkschlüssel M* sau *M3*. În timp ce armata folosea doar trei rotoare la acel moment, pentru a creşte nivelul de securitate, Marina a decis să folosească trei rotoare din cinci posibile.[21]

---

[18] Michael Smith Station X, patru cărţi (macmillan) 1998, Paperback 2000, Pag 73

[19] Kahn, 1991, pag 43

[20] Kahn (1991, pag 43) spune că în august 1934. Kruh şi Deavours(2002, pag. 15) spun că în octombrie 1934.

[21] Deavours and Kruh, 1985, pag. 98

În decembrie 1938, Armata a produs două rotoare suplimentare, astfel încât cele trei rotoare erau alese dintr-un set de cinci.[17] În 1938, Marina a mai adăugat două rotoare, şi apoi încă unul în 1939 pentru a permite alegerea a trei rotoare dintr-un total de opt posibile.[21] În august 1935, Forţele Aeriene au introdus Wehrmacht Enigma în comunicaţii.[17] Marina a introdus pentru traficul submarinelor o maşină Enigma cu patru rotoare, la 1 februarie 1942. Maşina se numea *M4* (reţeaua era denumită de Aliaţi *Triton*, sau *Shark*). Rotorul suplimentar a fost montat în acelaşi spaţiu prin reducerea grosimii reflectorului, ceea ce a făcut loc pentru un al patrulea rotor mai subţire.

A existat şi un model mare, cu opt rotoare şi imprimantă, numit *Enigma II*. În 1933, criptanaliştii polonezi au detectat că acesta era folosit pentru comunicaţiile militare la nivel înalt, dar că a fost retrasă din utilizare deoarece a fost considerată nesigură şi se bloca des.[22]

Enigma G, utilizată de Abwehr, avea patru rotoare cu marcaje multiple, şi nu avea tablou de prize.

Abwehr a utilizat *Enigma G* (*Enigma Abwehr*). Această variantă de Enigma era o maşină cu patru rotoare cu marcaje multiple, dar nu avea tablou de prize.

[22] Kozaczuk, 1984, pag. 28

Acest model era echipat cu un contor incrementat la fiecare apăsare de tastă, fiind astfel cunoscut ca *maşina cu contor* sau *Zählwerk Enigma*.

Maşina Enigma elveţiană, cu patru rotoare recablate, fabricată în Germania.

Şi alte ţări au folosit maşini Enigma. Marina italiană a adoptat varianta comercială ca "Cifrul Marinei D"; spaniolii au folosit maşina comercială în timpul războiului civil. Criptanaliştii britanici au reuşit să spargă aceste maşini, cărora le lipsea tabloul de prize. Elveţienii au utilizat o versiune de Enigma numită *model K* pentru comunitcaţii militare şi diplomatice, model foarte similar cu Enigma D. Maşina a fost spartă de mai multe ţări, printre care Polonia, Franţa, Regatul Unit şi Statele Unite (ultima a numit maşina INDIGO). Un model *Enigma T* (cu numele de cod *Tirpitz*) a fost fabricat pentru a fi utilizat de către japonezi.

Criptografia maşinii Enigma nu era perfectă, mai ales după ce aliaţii au capturat câteva exemplare, permiţându-le să decodifice mesajele germanilor, ceea ce s-a dovedit a fi vital în Bătălia Atlanticului.

S-a estimat că s-au construit în total aproximativ 100.000 de maşini Enigma.[23] După sfârşitul celui de-al doilea război mondial, Aliaţii au vândut maşinile Enigma capturate, şi considerate încă relativ sigure, unui număr de ţări în curs de dezvoltare.[23]

---

[23] Bauer, 2000, pag. 112

Enigma in zilele noastre

Efortul de a sparge maşina Enigma nu a fost dezvăluit decât în anii 1970. De atunci, interesul pentru maşinile Enigma a crescut considerabil şi mai multe exemplare sunt expuse astăzi în muzee din SUA şi din Europa.Deutsches Museum din München are versiuni militare cu trei şi patru rotoare, precum şi alte versiuni civile mai vechi. O maşină Enigma în stare de funcţionare este expusă la Muzeul Criptografic Naţional al NSA din Fort Meade, Maryland, unde vizitatorii pot să încerce să cripteze mesaje clare şi să descifreze mesaje codate. Armémuseum din Stockholm are şi el o maşină Enigma expusă. Sunt exemplare şi la Muzeul de Istoria Calculatoarelor din Statele Unite, la Bletchley Park în Regatul Unit, la Muzeul Armatei Poloneze din Polonia, la Australian War Memorial, şi în foaierul Defence Signals Directorate, ambele aflate în Canberra în Australia, precum şi în mai multe alte locuri din Germania, SUA, Regatul Unit şi în alte ţări ale lumii. Muzeul Calculatoarelor din San Diego, astăzi închis, avea în colecţia sa o maşină Enigma, pe care a dat-o apoi bibliotecii de la Universitatea de Stat San Diego. Altele sunt deţinute de colecţionari particulari. Ocazional, se vând maşini Enigma la licitaţii, la preţuri care ajung deseori la 20.000 de dolari.[24][25]

Replici ale maşinilor sunt disponibile în diverse forme, inclusiv o copie exactă reconstituită a modelului naval M4, o Enigma implementată cu circuite electronice (Enigma-E), precum şi diferite simulatoare software.

O maşină rară Enigma Abwehr, denumită G312, a fost furată de la muzeul Bletchley Park la 1 aprilie 2000. În septembrie, o persoană ce se autodenumea „The Master" a transmis o notă prin care cerea 25.000 de lire sterline şi a ameninţat că va distruge maşina dacă nu se plăteşte răscumpărarea. La începutul lui octombrie 2000, oficialii Bletchley Park au anunţat că vor plăti răscumpărarea dar termenul limită trecuse şi nu se auzise nimic de la şantajist. La scurt timp, maşina a fost trimisă anonim ziaristului BBC Jeremy Paxman, dar cu trei rotoare lipsă. În noiembrie 2000, un negustor de antichităţi pe nume Dennis Yates a fost arestat după ce a sunat la *The Sunday Times* pentru a face aranjamente pentru returnarea pieselor lipsă. Maşina Enigma a fost returnată la Bletchley Park după incident. În octobrie 2001, Yates a fost condamnat la zece luni închisoare după ce a recunoscut că a deţinut maşina furată şi că a cerut răscumpărare pentru returnarea ei, dar a continuat să susţină că era doar un intermediar pentru un terţ.[26] Yates a fost eliberat din închisoare după trei luni.

---

[24] Hamer, David; Enigma machines-known locations

[25] Hamer, David; Preţuri de vânzare ale unor maşini Enigma şi NEMA-convertite în dolari americani

[26] „Man jailed over Enigma machine". BBC News

Maşini derivate din Enigma

Enigma a avut o puternică influenţă în domeniul proiectării maşinilor de cifrare, şi mai multe maşini cu rotoare derivă din ea. Maşina britanică Typex a fost iniţial derivată din patentele Enigma; Typex include chiar şi caracteristici din descrierile patentului care au fost omise la realizarea practică a maşinilor Enigma. Din cauza nevoii de a păstra secretul asupra sistemului de cifrare, nu s-au plătit drepturi de autor pentru utilizarea patentului de către guvernul britanic. O clonă japoneză de Enigma a primit numele de cod GREEN de la criptografii americani. Folosită rareori, ea conţinea patru rotoare montate vertical. În SUA, criptologul William Friedman a proiectat M-325, o maşină similară cu Enigma din punct de vedere al funcţionalităţii, dar nu şi din cel al structurii.

O maşină cu rotoare unică a fost construită în 2002 de Tatjana van Vark din Olanda. Acest dispozitiv neobişnuit a fost inspirat din Enigma dar utilizează rotoare cu 40 de puncte, permiţând utilizarea de cifre, litere şi unele caractere de punctuaţie; fiecare rotor conţine 509 piese.[27]

O clonă japoneză de Enigma, denumită de criptografii americani GREEN.

[27] Van Vark, Tatjana „The coding machine”

Cuprins

În loc de introducere 1

Maşina de criptare ENIGMA 2

Descriere 4

Rotoarele 6

Schimbarea de stare 9

Roata de intrare 11

Reflactorul 12

Tabela de prize 13

Accesorii 14

Descriere matematică 16

Proceduri de folosire a Enigmei 17

Indicatori 19

Abrevieri şi moduri de lucru 21

Istoria şi dezvoltarea maşinii 22

Enigma “comercială” 23

Enigma “militară” 25

Enigma în zilele noastre 29

Maşini derivate din Enigma 30